COMS 4995-001 (Science of Blockchains): Homework #8

Due by 11:59 PM on Wednesday, April 16th, 2025

Instructions:

(1) Solutions are to be completed and submitted in pairs.

(2) We are using Gradescope for homework submissions. See the course home page for instructions, the late day policy, and the School of Engineering honor code.

(3) Please type your solutions if possible and we encourage you to use the LaTeX template provided on the Courseworks page.

(4) Write convincingly but not excessively. (We reserve the right to deduct points for egregiously bad or excessive writing.)

(5) Except where otherwise noted, you may refer to your lecture notes and the specific supplementary readings listed on the course Web page *only*.

(6) You are not permitted to look up solutions to these problems on the Web. You should cite any outside sources that you used. All words should be your own. Submissions that violate these guidelines will (at best) be given zero credit, and may be treated as honor code violations.

(7) You can discuss the problems verbally at a high level with other pairs. And of course, you are encouraged to contact the course staff (via the discussion forum or office hours) for additional help.

(8) If you discuss solution approaches with anyone outside of your pair, you must list their names on the front page of your write-up.

Problem 1

(10 points) Recall the selfish mining attack from the end of Lecture 21. Suppose a validator's utility was the *number* of blocks on the longest chain rather than the *share* of the blocks on the longest chain. Does the selfish mining attack from lecture (with ties always broken in favor of the adversary, like in lecture) still benefit the adversary? Either way, support your answer with a proof.

Problem 2

(15 points) Recall that the difficulty adjustment algorithm in Bitcoin uses the timestamps that miners place in blocks to measure the amount of real-world time used to add a batch of 2016 blocks to the longest chain, and then adjusts accordingly the proof-of-work difficulty for the next 2016 blocks.

1. (5 points) Suppose miners were free to put whatever timestamps they wanted into blocks. How could miners use this power to manipulate Bitcoin's difficulty adjustment algorithm and boost their rewards? Give a concrete example of an attack.

2. (3 points) Explain the rules that govern block timestamps in the Bitcoin protocol. (Cite the source(s) you used to answer this question; just the URLs are fine.)

3. (7 points) Discuss to what extent the rules in (2) mitigate the attack(s) that you described in part (1).

Problem 3

(15 points) For this problem, assume that all block timestamps are accurate. Different blockchains have different difficulty adjustment algorithms.

1. (4 points) Explain how the difficulty adjustment algorithm currently works in Bitcoin Cash, and explicitly compare and contrast it with the difficulty adjustment algorithm in Bitcoin. (Cite the source(s) you used to answer this question; just the URLs are fine.)

2. (6 points) Would the selfish mining attacks in Lecture 21 be more or less effective in Bitcoin Cash than in Bitcoin? Or are there arguments in both directions? In any case, justify your answer with examples and/or mathematical analysis.

3. (5 points) Discuss any additional pros and cons that you can think of between the Bitcoin Cash difficulty adjustment algorithm and that of Bitcoin.